jackson lewis
All we do is work.®

Key Action Items for Responding to Data Breaches

Data breaches—unauthorized access to or acquisition of personal information—require specific steps to address the incident. A summary of *some* key action items is listed below.

- **Investigate and review results.** Perhaps the most important item on this list, the company must determine how to obtain necessary information about the incident, such as conducting employee interviews or reviewing relevant activity logs. This action item often shapes what steps will come next. Investigation should focus on uncovering key information including: nature of incident and how it occurred; date incident occurred; date incident was discovered; total number of individuals affected; total number of individuals affected in each state, contact information for affected individuals, etc. It may be necessary to seek investigative assistance through third-party vendors, such as IT forensic experts.

- **Adhere to existing internal procedures.** The individuals responsible for responding to the incident should adhere to any existing company policies governing the breach response process. Additionally, the steps taken during this process should be documented appropriately.

- **Involve company leadership.** Ensure appropriate internal approvals are in place for incident response.

- **Coordinate with insurance.** Confirm whether insurance coverage exists and assess carrier's role in response.

- **Review agreements.** Review and confirm whether there are data security agreements in place with any vendors that will be assisting in the investigation and response to the incident.

- **Assess state/federal agency reporting requirements.** Document applicable complaint/report number(s).

- **Determine whether this is a reportable breach.** Consider industry, types of data, jurisdictions affected, potential for harm or misuse of information, and contractual obligations.

- **Consider whether the company will offer credit monitoring services.** While currently not required under the law, the company may want to consider the benefits of providing such services.

- **Set up call center.** Designed to respond to inquiries regarding the incident and escalate necessary concerns, setting up a call center often takes several days of lead time.

- **Prepare and send breach notifications.** Consider applicable federal and/or state requirements to provide notification to both individuals and relevant agencies, as well as requirements to provide notification to the three major credit bureaus. Many jurisdictions have specific notice content requirements. Also consider the manner in which the company will provide notifications (*i.e.*, via email, hard copy, or some other means).

- **Be prepared for complaints and agency inquiries.**

These are *some* key action items when dealing with a data breach—they do not include all necessary steps a company may need to take. They should be helpful, however, in providing a general guide to data incident/breach response.

For additional information, please contact:

Joseph J. Lazzarotti, CIPP
Shareholder | Morristown Office
973.538.6890 | lazzaroj@jacksonlewis.com

Jason C. Gavejian, CIPP
Shareholder | Morristown Office
973.538.6890 | jason.gavejian@jacksonlewis.com